WISCONSIN ServicePoint

Wisconsin's Homeless Management Information System, Wisconsin ServicePoint, has been in operation since 2001. The program provides a listing of resources for the public as well as a secure members' site for listing and updating available resources, vacancies, and training opportunities for clients and service providers. The HMIS utilizes secured Internet-based technology to assist homeless service organizations to capture information about the clients that they serve.

The HMIS website was developed in collaboration with the Bowman Systems and local homeless providers. The State of Wisconsin's Department of Commerce is the system administrator and the central server is administered by the software vendor, Bowman Systems. There is limited access to the database; access is granted only to programs participating in the project. As the host, the Department of Commerce provides technology, training and technical assistance to users of the system throughout the state.

The structure and processes needed to implement the HMIS and to bring Wisconsin into compliance with the newly published National Standards are outlined in the HMIS Standard Operating Procedure. The Standard Operating Procedure document provides the policies, procedures, guidelines and standards that govern the HMIS, as well as roles and responsibilities for participating agency staff. Participating agencies will receive the complete document. They are to remain in compliance with agency specific policies listed in the Standard Operating Procedure as confirmed in their signed Agency Agreement.

The benefits of the HMIS are to:

- Inform government and the community about the extent and nature of homelessness in the state and their local communities.
- Assist numerous planning processes.
- Enable agencies to have accurate information about the clients they serve.
- Provide information on successes and challenges of homeless programs.
- Prepare informational reports for funders.
- Facilitate getting funding for needed housing and other related services, thereby ultimately benefiting homeless households.
- Enable the agencies and the community to understand client needs, resources and gaps through the use of aggregated data.
- Help programs identify processes that are problematic, support redesign efforts, and improve the quality of the services provided by the organization.

GOVERNING PRINCIPLES

Data Integrity:
Data are the most valuable assets of the HMIS project. It is the policy to protect these assets from accidental or intentional unauthorized modification, disclosure or destruction. Our data security program must be a well-organized and cost-effective plan, which formulates the safeguards to protect client, agency and policy level interests. The Bureau of Housing staff is responsible for controlling access to the system and will authorize access to essential service sites and central server locations only, as permitted according to the procedures outlined in this document.

Access to Client Records:
Access to Client Records is limited and regulated in order to protect against the recording of information in unauthorized locations or systems. Privacy protection policies include:

- ❖ No client records will be client assent or pursuant to law.
- ❖ Client identifying information is stored in a secured Central Server.
- ❖ Client information transferred from one authorized location to another over the web is transmitted through a secure, encrypted connection.

Obligation for Client Access to Records:
Whether requested of the Bureau of Housing or a specific service provider, clients have certain rights pertaining to information specific to them.

- ❖ The client has the right to know who has entered information and from what agency. The client has a right to know what information is contained in their records and what agencies have provided it.
- ❖ The client has the right to not answer any question, unless entry into a service program requires it.

Computer Crime:
Computer crimes violate state and federal law as well as the Data Standards. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs, or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data, or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both.

Data Entry Ethics:
Users must not attempt to gain physical or logical access to data or systems for which they are not authorized.